Release Notes for RFS6000 v3.3.1.0-003R

Contents

1. Introduction
2. RF Firmware Versions & compatibility matrix
3. Installation Guidelines
   3.1. Upgrade Procedure
   3.2. Auto Install Procedure
4. Important Notes
5. Issues Resolved
6. Known Issues
7. Note on Cluster UI

1 Introduction

Wi-NG v1.3 is a minor feature release for Motorola's Enterprise-class RF & Wireless Switches that enables a Wireless Enterprise by delivering an extremely resilient, high performance network that ensures seamless & secure voice and data communications. WI-NG v1.3 maps to v3.3.1 on the RFS6000 platform.

Key features in Wi-NG v1.3 to include:

Resilient and High Performance Networks with:

- SMART RF Management provides the capability for automatic analysis, configuration, and monitoring to optimize an ever-changing RF environment
- Adaptive AP support for 802.11a/b/g/n AP7131 single and dual radio with v3.1.1 on the Adaptive AP

RF Networks **securing mobility** by providing:

- Rogue AP Containment
- Ad Hoc Network Detection
- .11n Rogue AP Detection
- Detect de-authentication from broadcast source MAC
- Detect frames with invalid sequence number

Quality of experience and Service for VoIP users

- TSPEC Admission Control

Other system enhancements in this release include:

For the Adaptive AP 5131(ADP image v2.2.1):

- Rogue AP detection
- Mesh statistics
- WLAN statistics
- Configurable IPS Sensor on the AP5131(D mode SKU) in Adaptive mode(ADP image v2.2.1)

With the AP300:

- Dynamic Load balancing of APs after a primary reverts in a cluster
- Email Notification for critical alarms
- Cluster GUI for WLANS and APs functionality
- Securing Layer 3 AP and Wireless Switch protocol - Secure WiSPe Protocol
- MU Naming
- IP v6 Client Support

In addition to the new features above, the following functionality have also been enhanced in this release:

LED blink pattern for locating AP300s

To locate a particular AP300 in that has been installed, the user can now make the AP300 flash its LED by using the following command:

```
"radio <index> location-led (start-flashing | stop-flashing)" commands under "wireless" context.
```

CLI command to show description fields for APs and Mobile Units

The user can customize the show command outputs for show wireless mobile-unit and show wireless radio:

```
RFS6000#service wireless custom-cli ?
  sh-wi-mobile-unit  customize the output of the "show wireless mobile-unit" command
  sh-wi-radio        customize the output of the "show wireless radio" command

RFS6000#service wireless custom-cli sh-wi-mobile-unit ?
  ap-locn     location of the AP where the mobile-unit is associated
  ap-name     name of the AP where the mobile-unit is associated
  channel     the channel of the radio where the mobile-unit is associated
  dot11-type  the dot11 radio type of the mobile-unit
  ip          the IP address of the mobile-unit
  last-heard  the time when a packet was last received from the mobile-unit
  mac         MAC address of mobile-unit
  radio-bss   the bssid of the radio where the mobile-unit is associated
  radio-desc  description of radio where the mobile-unit is associated
  radio-id    radio index to which the mobile-unit is associated
  ssid        the ssid of the mobile-units wlan
  state       the current state of the mobile-unit
  username    the Radius username of the user connected through this device
              (shown only if applicable and available)
  vlan        the vlan-id assigned to the mobile-unit
  wlan-desc   the wlan description the mobile-unit is using
  wlan-id     the wlan index the mobile-unit is using

RFS6000#service wireless custom-cli sh-wi-radio ?
  adopt-info  adoption information about the radio (whether its on current
              switch, or some other switch in a cluster)
  ap-locn     location of the AP to which this radio belongs
  ap-mac      MAC address of AP to which the radio belongs
  ap-name     name of the AP to which this radio belongs
  bss         the bssid of the radio
  channel     the configured and current channel of the radio
  dot11-type  the dot11 type (11a/11g etc)of the radio
  num-mu      number of mobile devices associated with this radio
  power       the configured and current transmit power of the radio
  pref-id     the adoption preference id of the radio
  radio-desc  description of radio
  radio-id    radio index in configuration
  state       the current operational state of the radio

EXAMPLE::: Customize the output
---------------------------------
RFS6000(config-wireless)#service wireless custom-cli sh-wi-radio ap-locn num-mu ap-mac channel power

RFS6000(config-wireless)#sh wireless radio
AP LOCATION        #MU AP MAC             CHANNEL  POWER
San Jose 1st floor  0    00-15-70-15-11-62  40 (40 ) 4 (4 )


EXAMPLE::: Back to default
---------------------------
RFS6000(config-wireless)#no service wireless custom-cli sh-wi-radio RFS6000(config-wireless)#sh wireless
radio
IDX   AP MAC             RADIO-BSSID       TYPE  STATE    CHANNEL  POWER  ADOPTED-BY
1     00-15-70-15-11-62  00-15-70-14-52-3C 11a   normal   40 (40 ) 4 (4 ) current-switch
```

NAS identifier

```
“nas-id” can now be globally set using the command: RFS6000(config-wireless)#nas-id "my-string"
 The user can also override the nas-id on per WLAN basis using: RFS6000(config-wireless)#wlan 1 nas-id
"my-string"
```

Configuration migration from WS5100:

For those customers who were previously on a WS5100 infrastructure with Wi-NG code, and are now migrating to the RFS6000, with the previously used configuration, please note the following changes that will apply:

On RFS6000 CLI, "eth1" is now an alias for "ge1" and "eth2" is an alias for "up1". The "running-config" and other

"show" command output where interface name is displayed (and all of Web UI) will not show "eth1" or "eth2" names.

New CLI command to view the Signal, SNR and Average Data Rate as a summary table for all Mobile Units

```
RFS6000#sh wireless mobile-unit statistics summary /--------------------+----+-----------------------------
-----------+-------------------------------------------\
|Mobile Unit Mac /    |    |           last 30 seconds               |           last 60 minutes
|
|       Name          |Wlan|Signal | Noise |  SNR  |Avg Rate |Retries|Signal | Noise |  SNR  |Avg Rate
|Retries|
+--------------------+----+-------+-------+-------+---------+-------+-------+-------+-------+---------+----
---+
|00-12-17-62-F8-31    |3   | -27.71| -92.14|  64.43|    6.00 |   0.00| -30.71| -92.71|  62.00|   38.15 |
0.01|
|00-18-DE-0C-6E-6D    |3   | -55.43| -94.29|  38.86|    6.00 |   0.00| -45.29| -94.14|  48.86|   14.43 |
0.00|
|00-15-AF-EF-1C-C7    |3   | -24.57| -91.43|  66.86|   54.00 |   0.00| -24.43| -92.43|  68.00|   53.51 |
0.15|
|00-07-40-FA-D3-85    |3   | -38.14| -84.43|  46.29|   54.00 |   0.00| -37.71| -90.86|  53.14|   46.63 |
0.06|
\--------------------+----+-------+-------+-------+---------+-------+-------+-------+-------+---------+----
---/
```

Note: Please note that RFS6000 v3.3.1.0-003R software update can be applied only to the RFS6000 switch.

2 RF Firmware Versions & Compatibility Matrix

Access Point/Access Port	Firmware Version
AP300	00.02-31
Layer 3 AP300	01.00-2144r
WIPS Sensor Image for AP300	00.00-04
AP100	02.05-00
AP4131	07.00-08
AP4131 Revert	00.00-00
Adaptive AP Image for AP-5131 (ADP image)	2.2.1.0-004R
Adaptive AP Image for AP-7131	3.1.1.0-001R

For the prior Wi-NG releases on the RFS6000, please see compatibility matrix with Adaptive APs below:

RFS6000	AP5131 802.11 a/b/g	AP7131 802.11 a/b/g/n
v3.1	v2.0	N/A
v3.2	v2.1	N/A
v3.3.1	ADP v2.2.1 (Separate image)	v3.1.1 (to be used only in Adaptive AP installations)

Note: Please upgrade Adaptive AP 51X1 from 2.1.to ADP image v2.2.1 to work with v3.3.1 on the RFS6000. Please be aware that for existing installations that have v2.1 on the AP51X1 as Adaptive, the v2.1 AP will not get adopted by the v3.3.1 switch but will appear in the 'un-adopted list' until user sets up the switch to push the ADP 51X1 v2.2.1 image.

3 Installation Guidelines

For accessing the Graphical User Interface (GUI) of the RFS6000 switches, the following browsers (and Java versions) are supported:

- Internet Explorer 6.0, 7.0 on Windows 2000, XP (JRE 1.4.2)
- Mozilla 1.4.3 on RedHat Linux (tested with JRE 1.5)
- Firefox 0.8 or higher on Windows 2000, XP (JRE 1.4.2)
- Firefox 1.0 or higher on RedHat Linux (tested with JRE 1.5)

3.1 Detailed Firmware Upgrade Procedure

This section outlines the upgrade procedure to v3.3.1 applicable if the RF switch had a beta release installed.

The method described in this section uses the Command Line Interface (CLI) and GUI and the Auto-Install procedures. To log into the CLI, either SSH, Telnet or serial access can be used (whichever exists).

Upgrading from a previous v3.x Beta or engineering build (v3.x.0.0-xxxB)

1. Copy the RFS6000_v3.3.1.0-003R.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

3.2 Auto-Install Process

Auto Install in v3.3.1 works via the DHCP server. This requires the definition of a Motorola Vendor Class and four sub-options under option 43 namely:

- Option 186 - defines the tftp/ftp server and ftp username, password information
- Option 187 - defines the firmware path and file name
- Option 188 - defines the config path and file name
- Option 189- defines the RFS6000 ip address to where a L3 AP300 RF port or Adaptive AP will be adopted
- Option 190 - defines the cluster config path and file name.

The individual features (config, cluster-config and image) may be enabled separately via the CLI, snmp or Applet. If a feature is disabled then it will be skipped when Auto install is triggered.

For the static case, where the URLs for the configuration and image files are not supplied by DHCP, the URLs may be specified via the CLI, snmp or Applet. The CLI may also be used to define the expected firmware image version. If the image version is not specified we will attempt to derive it from the file name, if it can not be derived from the filename then the system will simply attempt to load something other than what it is currently running.

Configuration files are tracked by their MD5 checksum, so if a file is renamed it will still have the same md5 sum. Once a file has been loaded it will not be reloaded, even if the local configuration information is changed.

The requested image file version, if any, is checked against the current version before any attempt is made to load it. If the requested version is the same as the running version then no further action is taken. If the image file version, embedded in the file header, does not match the expected version then no further action will be taken. If the version has not been specified then the header of the image file will be compared to the local version, if they are the same then no further action will be taken.

Please note that once the system has been operating for ten minutes, Auto Install is disabled, though it may still be reconfigured. This is to prevent the system from attempting to re-install each time a DHCP lease is renewed.

Configuring Auto Install via the CLI

There are three compulsory and four optional configuration parameters.

The compulsory parameters are:

- configuration upgrade enable
- cluster configuration upgrade enable
- image upgrade enable

Optional (only for the static case):

- configuration file URL
- cluster configuration file URL
- image file URL
- expected image version

The three enables default to yes, the URLs and the version default to "" (blank)

```
RFS6000(config)#show autoinstall

feature    enabled      URL

config       yes         --not-set--

cluster cfg  yes         --not-set--

image        yes         --not-set--

expected image version  --not-set--
```

The three enables and the expected version affect any mode of operation; the URLs are only used for the static (non DHCP option) mode.

Enables are set using the **autoinstall <feature>** command:

```
RFS6000>enable
RFS6000#conf t
RFS6000(config)#autoinstall image
RFS6000(config)#autoinstall config
RFS6000(config)#autoinstall cluster-config
```

After this configuration, any switch reboot with DHCP enabled on the port will trigger Auto Install, provided the DHCP Server is configured with appropriate options.

After the reboot switch would try to acquire the IP address from DHCP server. The DHCP server will provide the auto-install parameters like image, config and cluster-config files and paths provided if they were configured in DHCP server. Based on the parameters switch downloads the corresponding files from the specified server and reboots the box again in order to take effect the newly downloaded configurations. After the switch auto-reboot, the config and cluster-config (whichever) downloaded as part of auto-install will be applied to the switch becomes switch's running-config.

NOTE: The cluster-config will be applied to the running-config but not auto saved to the startup-config. If user wants to reboot the box again for any reason, must save the running-config using the command "write-memory". Otherwise on the next boot, switch will have only the startup-config and not the cluster-config in running-config.

The "enables" are cleared using the **no autoinstall <feature>**

URLs and the version string are set as text and can be cleared by using an empty pair of double quotes to denote the blank string. In the following example we define the three URLs and the expected version of the image file and then enable all three features for Auto Install.

```
RFS6000(config)#autoinstall config url
ftp://ftp:ftp@192.9.200.1/RFS6000/config
```

```
RFS6000(config)#autoinstall cluster-config url
ftp://ftp:ftp@192.9.200.1/RFS6000/cluster-config

RFS6000(config)#autoinstall image url
ftp://ftp:ftp@147.11.1.11/RFS6000/images/RFS6000.img

RFS6000(config)#autoinstall image version 3.3.1.0-003R

RFS6000(config)#autoinstall config

RFS6000(config)#autoinstall cluster-config

RFS6000(config)#autoinstall image

RFS6000(config)#show autoinstall

feature    enabled      URL

config       yes        ftp://ftp:ftp@192.9.200.1/RFS6000/config

cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/RFS6000/cluster-config

image        yes        ftp://ftp:ftp@147.11.1.11/RFS6000/images/RFS6000.img

expected image version  3.3.1.0-003R
```

Once again, for DHCP option based auto install the URLs will be ignored and those passed in by DHCP will not be stored.

Whenever a string is blank it is shown as **--not-set--**.

4 Important Notes

1. The **switches in the cluster need to have a Unique/different SNMP Engine ID for Cluster-GUI** to work. After the SNMP Engine ID is changed to be unique, all switches in the cluster need to be rebooted for the change to take effect. For customers using RFMS 3.0 or MSP 2.9 with SNMP v3, you may need to rediscover your network, after changing the Engine IDs to be the same again.
2. For customers using WMM-TSPEC clients, please enable through CLI: *wireless admission-control voice enable.*
3. If the user is not enabling SMART RF, but would like to share AP power and channel information across a cluster of switches, please enable through CLI “cluster master support enable”. If the user is enabling SMART RF, then this CLI command is enabled automatically, the user does not need to enable it.
4. For existing customers that were using Self Healing, Motorola has now introduced the SMART RF functionality. Both features cannot be used simultaneously. Please note that SMART RF also provides Neighbor recovery and Interference Avoidance.
5. For the Adaptive AP, ***the Independent and Extended WLANs must be on unique VLANs***.
6. For the Adaptive AP 7131, Mesh, L3 Mobility, Rogue AP Detection and WLAN Bandwidth Management are not supported on the Wireless Switch, when in Adaptive AP mode; for the Adaptive AP5131, with this v3.3.1 release, Rogue AP detection is supported on the Adaptive AP5131 with the ***ADP5131*** v2.2 image.
7. With the Adaptive AP, the number of VLANs/WLANS supported is 15.
8. Please be aware that on a hotspot authentication success page, pressing backspace on the screen restarts the time elapsed counter. However, session timeout at the back end will still remain the same.
9. In case of login issues to the applet, it is recommended to clear the java cache for the browser
10. ***When manually adding radios for Adaptive APs on the wireless switch, please specify AP5131/AP7131 where appropriate. The AP 300 is the default value.***

5 Issues Resolved

SPR	DESCRIPTION
16481	Security vulnerability – possible access to system thru CGI
16482	Security vulnerability – possible access to system thru CLI
16452	Hotspot and trusted WPA WLANs co-existence problems on ADP5131.
16478	Wireless Switch with large number of ADP5131 connected crashes unexpectedly with out of memory errors
16581	PSK-WPA2-TKIP is not working with Intel 4965ag and Broadcom a/b/g internal WLAN adapters with ADP5131 and AAP7131
Bug ID54835	Some ADP5131s do not re-adopt properly after switch fail-over.
Bug ID 54834	Prevent sending roam notification over the air.
15064	Similar credentials for log on can be used multiple times simultaneously.
15841	Frequent "%KERN-3-ERR: hub 1-1:1.0: over-current change on port 1" messages are seen
15883	LED behavior change with AP300 found in v3.2. Prior to firmware 3.2 the AP300 LEDs would only react to data transmitted or received on its own BSSIDs. The LEDs would only flicker when data was moving through the AP radios to the switch. In firmware 3.2 we introduced a new locationing feature. The addition of the new locationing feature is what has caused the LED status change. With this new feature the 802.11g radio is reacting to all BSSIDs in the environment rather than just its own. In areas where there are many wireless networks detected the LEDs will flicker non stop even when there is no data going through the APs to the switch. This behavior has now been corrected.
15926	LED Sequence for Fan and Temperature do not match documentation.
15958	Incorrect display of DHCP IP Address for wireless sensor.
15934	Wireless Switch is not able to connect more that 32 AAPs with dual radio.
15995	Radius Accounting log not available in 3.2
16013	The GUI does not present proper bandwidth allocation per WLAN
16057	AP-5131 operating as AAP will not beacon or respond to probes for 32 character SSID.
15148	Some of the v3.x switches have different engineid for the snmpmanager, snmptrap, and snmpoperator, thus causing problems during configuration import.
15260	When a device such as CA50 is involved in a VoIP phone call reaches an end of coverage area, devices close to AP not involved in the call are starved for data.
15576	Changing from WMM mode to Normal on switch, AP reports data for traffic with TIM bits set. When clients do a PS-Poll AP reports no data but continues to advertise TIM with data.
15587	– 426 Error received when pulling config from Windows 2000 IIS FTP
15674	A user who has Monitor only privileges is able to access enable mode and view the running-config.
15683	GUI Login Error User Authentication Failed Too Many Log-ins From The Same User
15835	When you do a 'show wireless radio statistics 6' the switch is interpreting the 6 as 60min instead of the radio index.
15856	Redundancy issue with TCP port when primary and standby switches are separated by a firewall. Documentation has been updated to reflect correct port range for firewall.
15882	AAPs do not show up in Unadopted List
15891	When you set the country code in the CLI to either JJ or JW the beacon transmits that same country code. Instead it should transmit JP as the valid country code in the beacon.
15954	If both options (43 & 189) are set in the DHCP scope, L3 adoption of AP300 is not working.
15992	Ports Down after start-up when MSTP instance name not 'My Name'
16025	Wireless Switch DHCP server wrong SVI (VLAN interface) IP association
16098	Internal DHCP server set to infinite lease time offers lease expiration date ending in year 1901.

SPR	DESCRIPTION
16156	Invalid RADIUS shared secret being pushed to adaptive AP-5131's.
16159	Doubling of the roam notifications are being generated on every roam during association and re-association.

6 Known Issues

CRID	DESCRIPTION	Resolution/Workaround
SPR 15628/15925	Multiple errors generated on the applet when accessing access port radio screen with a variety of different model laptops.	
SPR 16137	CPU load error message encountered under release 3.2	
SPR 16143	Telnetting to active cluster switch during extreme load - cli sometimes does not respond .	Please reboot the Switch.
SPR 16292	A tagged (VLAN) port accepts only tagged packets, it does not accept untagged packets	
SPR 16310	Password-encryption secret stays encrypted even after deleting startup-config and restoring switch to factory default	
SPR 16323	FW 3.2 - NTP is enabled and functional but the switch GUI shows it is disabled.	
SPR 16330	3.2 Internal FTP server access denied - missing support for NLST command	
SPR 15573	Wireless Filter CLI accepts range of 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF – this functionality is available through the CLI. There is a GUI mismatch.	
SPR 16099	Port Aggregation feature missing in the current version of the RFS6000	Release in H109.
44103	Adaptive AP: UAPSD parameters are not displayed for Mobile-devices associated to an Adaptive-AP.	This is only a GUI issue, UAPSD is enabled on the back end
52588	Cluster GUI: when enabled though GUI, the configuration is not in running config	The "Enable Cluster GUI" flag is valid only for the session as long as the applet is open. The moment one closes the applet, one is no longer in the Cluster GUI mode. The paradigm used here is similar to that present in cli. When one logs into a switch, one has to enter enable -> conf t -> to get into the default mode, then to enter cluster cli mode one has to explicitly enter cluster-cli mode. But after one logs out of the switch, and then reconnects they will have to again start from the default mode.
52517	Roaming of TSPEC MUs: Roamed MUs are admitted even when the configured max-roamed-mus count is zero and res-roam-perc is zero	The behavior is as expected. The roaming count of MUs and air time is used only when the radio has completely exhausted the max voice air time or has max MUs associated to it which are sending voice traffic. In this scenario, the max percentage is configured as 75% and max MUs is 2 on the new radio and hence it would accept ADDTS from 2 roamed MUs
52892	Enabling a new Wlan causes disassociation of all MUs connected to different WLAN with Manual WLAN mapping	Any config push to the AAP causes it to bring down all radios and reinitialize
52592	Cluster GUI: Customer cannot edit radio configuration for AP's not adopted.	

CRID	DESCRIPTION	Resolution/Workaround
52572	Voice stats: Calls per radio (current) does not get updated and other call stats are all wrongly displayed	MUs are initially associated as regular MUs. Only when they send any voice traffic they are identified as voice MUs so until the call is established these MUs will not show up as voice MUs. And these will be considered as voice MUs until they are reassociated and hence the current call, calls max and calls average never change until the MUs are reassociated.
52687	Wireless: cli command "dhcp-one-portal-forward" prevents CB3000 wired clients to receive DHCP address	Please disable dhcp-one-portal-forward command
53772	MU MAC name should not exceed 63 characters in the GUI	Will be fixed in the next release.
41870	Rogue AP: Duplicate entries are recorded in the Approved and unapproved AP list if two detectors detect the same AP.	
45167	Adaptive AP: Hotspot configuration for Independent WLANs on an Adaptive-AP cannot be configured from the switch.	The configuration does get pushed for the extended WLAN and therefore allows for a centrally configurable and manageable hotspot.
43606	User Account with a (') character in password causes login failure	Please refrain from using (‘) special character in the switch login password
44971	Adaptive AP: Adaptive AP cannot be adopted using the secondary IP address of a Switch Virtual Interface (VLAN interface).	Please use the primary IP address
39446	Console hangs in the case of excessive static NAT entries	System is fine with up to 128 NAT entries but there is a 15 second delay
39653	Switch console may hang for 20 minutes when large configuration file is copied to running config	When you load large configuration by copying to running-config, it may be slow. The recommended approach is to copy to startup config and reload the switch - this is much faster.
37280	Not possible to clear the DDNS IP bindings from the switch from CLI,APPLET and SNMP	The work around is that the DNS server which is managed by IT can clear the database using separate commands The work around is that the DNS server which is managed by IT can clear the database using separate commands.
40183	Network > Access Port Radios > WLAN Assignment page display incorrectly and "Index" filter not functioning	This only happens when the user is frequently switching between tabs. A refresh of the screen displays the right values.
37592	The discovered switches are lost after a reboot	Work around: If you just reload the switch and keep the browser open the dropdown box with the other switches IP will remain.
39552	IP address in with leading zeros aaa.bbb.ccc.ddd format to a target server (to transfer a file or firmware) is not working i.e. 192.168.2.1 works but not 192.168.002.001	To be resolved in a future release

CRID	DESCRIPTION	Resolution/Workaround
40110	Radius server restart to pick up configurations changes takes 2 minutes if 5000 radius users are present.	The config change will be picked up, but it takes 2 minutes for radius service to start itself once it had stopped to pick up the config changes. During this period any eap authentication or hotspot authentication tried will get failed.
37094	No option to enable portfast on interface from applet	Can be applied through CLI: In CLI int ge1# spanning-tree port-fast
36996	Changing username/password for AP port authentication doesn't take effect immediately.	A reset or power off/on is currently required.
50494	AAP: Hotspot authentication for independent WLAN, using AP5131's on-board RADIUS fails	Please use an external RADIUS or the Onboard RADIUS on the Wireless Switch.
50187	Detector APs may reboot when browsing through the Rogue AP report.	No network disruption, as this only affects detector mode APs.
48343	AAP/applet: User cannot select AP image from the GUI on AAP firmware page, for USBs.	The following USBs have been tested to work and do not have the problem: • Memorex traveldrive 2.0GB (USB 2.0) • Kingston DataTraveler 1.0BG • Memorex traveldrive 8.0GB (USB 2.0)
48882	AAP FW Upgrade failed when upgrade file is on cf and ftp root dir is also cf	The upgrade image has to be named as "aap_fw_image" and be present in the root of cf or usb and the same external drive has to be configured as the ftp root to get this working.
48915	IPSEC - ISAKMP Aggressive mode settings doesn't works	This can be configured as follows to work: On SW1(IP 10.10.10.45) ======-========== crypto isakmp key 0 test12345 address 10.10.10.250 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.250 match address aclstos set mode aggressive set transform-set tfset On SW2 (IP10.10.10.250) ========== crypto isakmp key 0 test12345 address 10.10.10.45 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.45 match address aclstos set transform-set tfset set mode aggressive
48827	USB: Drive mapping changes when an USB Flash drive is unplugged and plugged back while data transfer is in progress	Please do not unplug the USB while it is in process.
50469	Hotspot+Guest user+Applet: Not able to create Guest user when switch time is 00:00 (24hr format) from Applet	Guest user will not be created and it will display error as "switch date should be greater than current switch date".
49342	AAP: Deleted AAP radio will not be adopted after enabling adopt unconfigured radio.	This can be recovered by doing the following: • Delete the AAP. • Reboot the AAP. • Reboot the switch.

CRID	DESCRIPTION	Resolution/Workaround
49356	RTLS: 'reader 1 antenna 1 power' doesn't really apply to the third party reader	Please set power levels directly on the reader.

7 A Note on Cluster UI

Once a user enables 'Cluster GUI' on the Redundancy page (under Services sash), the user will be in the cluster GUI context similar to the 'cluster-cli' context (provided the 'Enable Redundancy' option is turned on too. This context lasts until the user is logged in and will be lost every time a user logs out of the GUI (similar to what is done in the cluster cli - the context is lost when a user logs out of the switch).

If the 'Enable Redundancy' option is deselected, automatically the 'Cluster GUI' option will be disabled.

One can see the switches participating in the Cluster GUI by seeing the 'Member' tab in the 'Redundancy' page (Services -> Redundancy). The 'Status' has to show 'Established' as well against each member switch. If a 'Not Seen' is displayed against the status, then the switch will not be displayed in the cluster GUI.

Functionality supported with the Cluster UI

a. Wireless LAN(under Network sash, choose Wireless LAN and the Configuration tab)

Operations supported are:

Display: The data will be fetched from all the switches in the cluster and will be sorted based on the index value. One will see the additional Switch column to the left to distinguish data from each switch.

Note: If this page was clicked for the first time after the 'Cluster GUI enabled' checkbox was selected, then there will be a time delay until the data loads completely. This happens only for the first time since each of the Switches needs to be logged into (only for the first time). This time delay is proportional to the number of switches in the cluster times 5 seconds. It is necessary that all the switches are reachable from the current switch (If not, a message will be shown to the user saying that a particular switch is not reachable and hence data will not be fetched for it).

Configuration: On selecting a single row and clicking 'Edit', it will bring up the Edit dialog. When one edits a couple of fields in the dialog and clicks on 'Apply To Cluster', it (only the changes made) will be applied to all the switches in the cluster.

If one wants to only apply changes on this particular switch only, one can click on 'OK' button.

The sub dialogs for instance the 'Config' button against the Encryption type 'WEP 64' contains its own 'Apply to Cluster' button (this is for applying the data on the sub dialogs across the cluster).

Note: On multiple select of rows (belonging to different switches, the 'Edit' button will not be visible), however on multiple select of rows belonging to the same switch, the Edit button is enabled and the Edit dialog will display common fields that can be edited across multiple WLAN entries pertaining to the selected switch and in this case the 'Apply To Cluster' button is disabled.

Enable/ Disable option on selecting multiple rows works as before and is allowed across different switches too.

Currently, the 'Global Settings' button is not supported for cluster mode, nor are the other tabs under Wireless LAN apart from the Configuration tab.

b. Mobile Units (under Network sash, choose Mobile Units and the Configuration tab)

Display: Same as Wireless LAN.

Configuration: Since the only editable field in this page is the MAC Name, one can edit the field on different rows belonging to different switches (one at a time) and then click on 'Apply' finally.

c. Access Port Radios (under Network sash, choose Access Port Radios and the Configuration tab)

Display: Same as Wireless LAN.

Configuration: Similar to Wireless LANs. However, since the AP Radios have different indexes on different switches, the changes applied will be seen on the corresponding AP Radio on the corresponding switches in the cluster (sharing the same MAC Name but may have different indexes - so this may appear different).

Add - One can either add an AP Radio to this switch or across multiple switches.

One can select multiple rows and click on '**Delete**' option to delete AP Radios across switches in the cluster.

Note:

The 'Global Settings' and 'Tools' button are unsupported as of now in the cluster mode.

Since the 'Group ID' belongs to a single switch, one cannot apply it on the cluster.

Other details:

On each of the first pages(in the Configuration tab for cluster supported pages), there is an option where a user can select a particular switch and see data corresponding to the selected switch or can choose 'All' to view data from all switches. One can see this option only from the first pages and. This option will not appear on subsequent pages, since paging is not supported for data fetched from a particular switch using this option.

On clicking the 'Save' button besides the Logout option; one can save the data from the running-config to the start-up config for all the switches in the cluster.

Some Known Issues:

- Sort is supported only on the data on a single page and not across the entire set of data.
- Sometimes there is a refresh problem and certain rows may appear missing, a click on 'Refresh' should solve the problem.
- It is necessary for the switches to have different Engine IDs for the cluster GUI feature to work properly. One will see issues after a reboot of any switch sharing the same engine id with another switch. In this case, data will be loaded only from one of the switches and leads to inconsistency.
- If one is using the discovery option and choosing between different switches (in the 'Connect To' option from the 'Login Details' on the left bottom corner of the main panel), then one will always see the message "Cluster GUI is being enabled" for the cluster supported pages. This will not be shown if you browse pages on the same switch thereafter.
- A maximum of 20 sessions can be open to the same switch (due to SNMP v3 security restrictions).
- Cluster GUI is not supported in a NAT'ed environment.